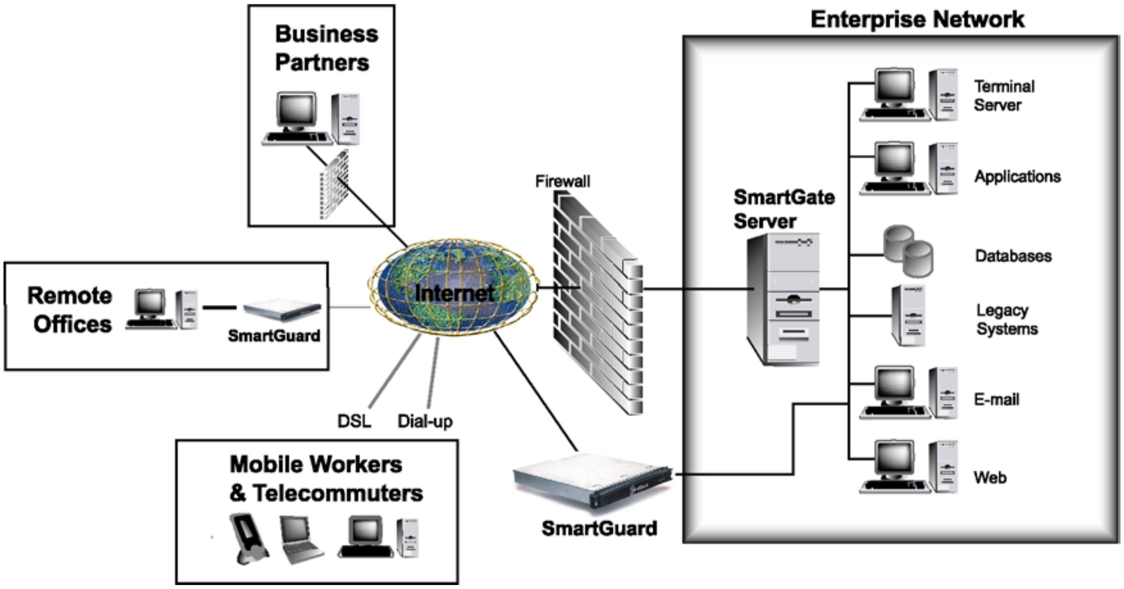
V-ONE TECHNOLOGY

How It Works

White Paper

EXECUTIVE SUMMARY

V-ONE Corporation's patented technology and state-of-the-art products are designed to protect information during Internet transport. V-ONE's SmartGate®, SmartPass®, SmartGuard™, and Air SmartGate™ client/server security software comprises an all-encompassing solution for enterprise-level security. V-ONE's solution keeps information private and provides services to a global network of users. In addition to strong and transparent security for TCP/IP-based applications, and IPSec tunnel functionality that encapsulates, encrypts, and protects data from examination or modification, SmartGate also supports encrypted wireless data transfer for pagers. Distributed worldwide, SmartGate ensures authentication, authorization, strong encryption, key distribution, proxy capabilities, IPSec transport functionality, accounting, data integrity, and non-repudiation.



Virtual private networking (VPN) options today span multiple encryption schemes and implementation techniques. SmartGate implements the security policy: "access is forbidden unless explicitly permitted." The default encryption method is 3DES (Triple DES), the strongest encryption level widely used by the U.S. Federal Government. It is applied both to verify the user's identity and to protect the flow of data.

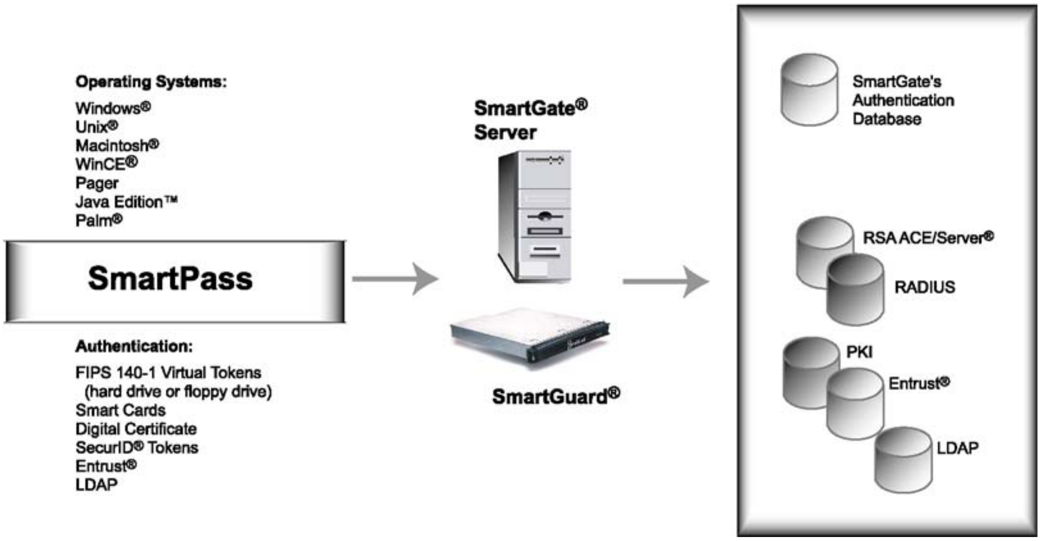
V-ONE's patented On-Line Registration (OLR) provides the ability to securely register users in seconds via the Internet. All registration information is secured by 3DES encryption. Once a registrant is enabled, access permissions are dynamically downloaded, and kept on the client machine only for the duration of the session. Access is based on authenticated user identification, independent of the source IP address. Every user can be allowed access to entire networks, certain applications, specific URLs and other resources. Management of thousands of users can be accomplished locally or remotely using the Web administration tool, SmartAdmin. Moreover, by using the SmartGuard Command Center, an administrator can securely manage thousands of SmartGuard appliances from one location.

V-ONE's implementation of IPSec is a traditional, standards-based IPSec client application that supports the IPSec protocols defined in RFCs 2401 through 2412. It operates at the network transport layer and requires changes to the Windows® device drivers. IPSec supports all IP applications and offers "same as on LAN" network services.

In addition to IPSec, V-ONE's method of implementing fine-grain data protection relies on an application proxy. The server sits between the user and the applications on, behind, or parallel to the firewall and acts as a proxy server. After mutual authentication (the server to the client and the client to the server), a session encryption key is exchanged and the server acts as a proxy by intercepting the data. The server then verifies that the data is permitted to be sent to the destination requested. Each time a session begins, a new key is automatically generated preventing decryption by unauthorized users. A single visit to a URL could result in multiple encrypted sessions—one for each file contained in a Web page.

V-ONE's server products support Microsoft Windows, Linux and UNIX operating systems and the client software supports Windows, UNIX, Macintosh, Windows Pocket PC/CE, Palm, pager, and the browser-based Java™ programming language. SmartGuard is available on a hardened kernel version of Red Hat® Linux that includes a stateful inspection firewall.

SmartGate supports the widest range of authentication methods—a FIPS 140-1 validated virtual token, ISO standard smart cards, RSA® SecurID® tokens, RADIUS®, Entrust®, Public Key Infrastructure (PKI), Lightweight Directory Access Protocol (LDAP), and a browser-based Java™ client.



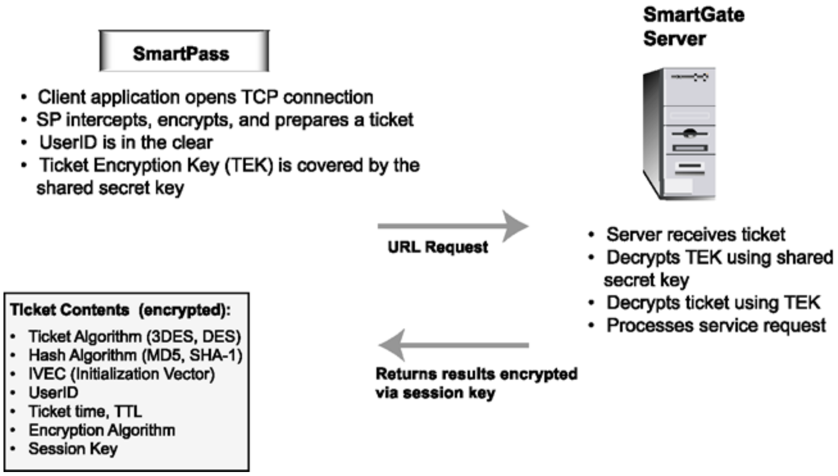
Although SmartGate alone is a complete solution for sensitive/confidential communications, it can be seamlessly integrated with a wide range of network security products. Ease of deployment, simple management, and scalability are just three of the exceptional features that propel SmartGate to the forefront of the virtual private network market.

V-ONE TECHNOLOGY

Some of the capabilities of the V-ONE technology are explained below.

SmartPass Client

Installation and operation of the SmartPass client software is entirely non-intrusive. After installation, when SmartPass is initially launched, a unique authentication key is generated. The authentication key is stored on the user's smart card (physical or virtual) and in the SmartGate server's user database. After SmartPass prompts the user to enter his access code, the identification and authentication process begins. SmartPass opens a TCP connection and prepares a ticket that contains the data required for authentication. The ticket is encrypted with a one-time Ticket Encryption Key (TEK), which is itself encrypted with the user's shared secret key. The user's ID, the TEK, and the ticket are then sent as a package to the SmartGate server. When these are received by the server, it retrieves the user's shared secret key, decrypts the TEK, and finally decrypts the ticket itself. The server then processes the service request and returns the results encrypted with a newly generated 3DES session key. Each client TCP connection generates a new authentication ticket and each client TCP connection has a unique session key.


SmartPass
• Client application opens TCP connection
• SP intercepts, encrypts, and prepares a ticket
• UserID is in the clear
• Ticket Encryption Key (TEK) is covered by the shared secret key
SmartGate Server
URL Request
• Server receives ticket
• Decrypts TEK using shared secret key
• Decrypts ticket using TEK
• Processes service request
Ticket Contents (encrypted):
• Ticket Algorithm (3DES, DES)
• Hash Algorithm (MD5, SHA-1)
• IVEC (Initialization Vector)
• UserID
• Ticket time, TTL
• Encryption Algorithm
• Session Key
Returns results encrypted via session key

When the SmartPass client is launched, it automatically contacts every SmartGate server for which the user has an authentication key and requests the user's current access permissions. The access permissions are created and controlled by the SmartGate administrator. The SmartGate server(s) returns the user's current access permissions to the SmartPass client. The user's access permissions are dynamically updated at startup and at regular intervals. No permissions are kept in permanent storage on the client desktop.

Every encrypted session, as well as the identification-authentication-Dynamic Configuration sequence occurs within seconds, indicated to the user by a small gold lock appearing over the SmartPass icon in the taskbar during the transmission of encrypted data. The user can remain uninvolved in this entire sequence or, if more technically astute, he can double-click the SmartPass icon to display the user interface and observe the connection progress as it is established and used.

SmartPass can employ either the Winsock Shim or localhost proxy. V-ONE's TCP/IP encryption technology does not interfere with the installed Winsock library. Instead, we install a Layered Service Provider (LSP) and a Name Service Provider (NSP), which work in cooperation with the Winsock library.

On-Line Registration (OLR)

SmartGate's patented OLR capability allows end users to register via the Internet and begin utilizing SmartGate-secured applications within minutes. By default, the user is required to complete two fields, which together form the user's long name in the user database. However, up to eight custom data registration fields per OLR method can be defined by the administrator to gather specific information from the end user—for example social security number, rank, company name, title, or e-mail address. The administrator can also have the user select his user group from a list of groups with previously assigned group-specific access permissions. The SmartGate administrator can also brand the OLR Web page with company-specific information.

The user performs OLR after installing and launching the SmartPass software, during which time the user must define and enter his access code. The SmartGate administrator maintains control over access code content and length criteria. The SmartGate administrator can configure the SmartPass Client installation software to automatically launch the user's Web browser directly to his company's OLR Web page immediately after installation, or the URL can be manually deployed to the end users. The OLR Web page for the specified SmartGate server will be displayed in the browser; in this Web page, the user enters the required data and clicks "Register." The SmartGate server displays an OLR success Web page containing server information and UserID. UserIDs are automatically generated during OLR without interaction from an administrator. Alternately, a UID server can be used to assign specific administrator-controlled UserIDs.

After a user has successfully registered and has been enabled by the administrator, SmartGate dynamically pushes the user's current access permissions down to the SmartPass client. These access permissions are not stored permanently on the user's computer.

Single Port Proxy Capability

The SmartGate Single Port Proxy provides the various SmartGate services with a single port presence on the network. This means that all SmartPass-to-SmartGate (client-to-server) connectivity will pass through the Single Port Proxy, and be forwarded to the correct destination service. The Single Port Proxy determines the service destination for each SmartPass connection using a port-mapping file with a default set of rules. These rules are configurable by the SmartGate administrator.

SmartGate Aware

An additional feature of the SmartGate server allows SmartGate-secured proxy services [Generic (sgate) and HTTP (sweb)] to receive information about SmartGate users accessing these services. A service that receives such information is referred to as being "SmartGate Aware." For example, if the SmartGate authorization process, which is a pass/no pass function, is not sufficient for special client applications, SmartGate can pass authenticated authorization information (i.e., UserID, name, user group, etc.) to the client application. SmartGate Aware is supported by the following services:

- **Generic Proxy (sgate) Services**—The generic proxy supports handshaking protocols, in which information is passed to the client/server, and SmartGate waits for a response. The VONE (default) and VPOP protocols are currently supported. The VONE protocol is defined as a simple "send message–wait for response" handshake between sgate and the client/server. The VPOP protocol is the method by which the Post Office server becomes SmartGate Aware.

- **HTTP Proxy (sweb) Services**—The Web proxy supports information-only protocols, in which information is passed to the client/server but SmartGate continues to pass the data. In this case, SmartGate Aware is used to monitor which Web sites people are accessing.

V-ONE's IPSec Implementation (IPSec)

IPSec's Core Components

There are two types of data encapsulation available with IPSec that can be employed individually or in combination:

1. Authentication Header (AH)

AH adds a digital signature to the IP header using the Message Digest (MD) or the Secure Hash Algorithm (SHA). AH authenticates the packet and assures data integrity by enabling detection of any alteration during transmission. AH provides a packet-by-packet authentication of the entire data stream, including the IP headers. AH can be applied alone, but is usually applied in conjunction with Encapsulating Security Payload (ESP). Although the AH authentication can add a significant level of security to ESP, it does not work in situations where intermediate gateways on the network perform Network Address Translation (NAT). NAT modifies the IP header that will render the hash incorrect and cause the packet to fail authentication. V-ONE's AH supports MD5-HMAC and SHA-HMAC authentication hashes. Basically, MD5 is faster, whereas SHA is cryptographically stronger.

2. Encapsulating Security Payload (ESP)

ESP encrypts and decrypts either the data or the entire packet using DES or 3DES encryption. ESP keeps transmitted data strictly confidential, and can provide adequate data integrity for most applications. ESP provides the encryption part of IPSec, as well as optionally calculating a packet-by-packet authentication hash of the payload of each packet (but not of the IP headers). V-ONE supports DES and 3DES encryption types in ESP, and SHA1 and MD5 authentication hashes. Using V-ONE's IPSec, each user can be set up with a different type of tunnel that allows access to different parts of the network using different levels of encryption/authentication.

IPCOMP—IP Payload Compression

IPCOMP is a method of compressing the data in the payload of an IP packet so that it will take up fewer bits on the wire. V-ONE supports the DEFLATE protocol. When compression is selected, an attempt is made to compress each packet that is more than about 100 bytes long. If the resulting packet is not shorter, the original packet is sent; otherwise, the compressed packet is sent.

NAT—Network Address Translation

NAT translates the IP addresses on a packet as the packet passes a gateway (in this case, the SmartGate Server). NAT has many uses, the most common being to allow a large number of hosts to share a single IP address [another name for this use is NAPT (Network Address and Port Translation) and 1:N NAT]. V-ONE does not use NAT for this purpose. V-ONE's NAT is a "1:1" NAT, and it is used for two reasons:

1. It provides each remote personal computer with a known IP address on the protected network.
2. It allows the SmartGate server to be located on the network "off to the side" from the natural route from the protected servers back to the clients on the Internet. Thus, SmartGate cannot become a "single point of failure" for the network.

Currently, SmartGate only NATs the client's address, and each client is assigned a unique address while it is connected. This eliminates many of the problems associated with 1:N NAT (where all clients would share the same IP address on the protected network). For example, if 1:N NAT were used, it would not be possible for others to mount the drives on remote clients, but this is possible in the V-ONE system.

An important note: currently, the NAT address for each client is assigned automatically from a pool of addresses when the client authenticates and does Dynamic Configuration. This address remains allocated to the given client not only until the client disconnects, but also until the server is restarted. Thus, the administrator must allocate a pool of addresses large enough to provide a unique address for every user (not just every simultaneous user).

IPSec in Operation

To send data to another machine, an application on the client calls the Winsock with some data. Winsock, in turn, passes this data down to the Microsoft Windows IP module, which breaks the data up into packet-sized chunks, adds an IP header (containing information about source and destination addresses, protocol, port, length, etc.) to the data, and sends it down to the next lower layer. Normally, the next layer is the driver for the network adapter card; but when

V-ONE's IPSec is installed, the packet is instead sent to the IPSec layer. IPSec compares the packet to an access control list (ACL) that it was given during Dynamic Configuration, and determines whether the packet should be encapsulated (tunneled, encrypted, etc.) and where the packet should be sent.

Additional protocol support

IPSec can carry **any** IP traffic—TCP, UDP, ICMP, or any other IP protocol. This means that remote users can share disks and printers using Microsoft® networking and browse Microsoft® Windows® Network Neighborhood.

SmartPass JAVA™ Edition Client

The Web browser–based SmartGate's Java Client (SGJC) emulates most of the functionality of the installed SmartPass client without requiring the end user to install any software on his desktop.

SGJC also does not require the user to perform OLR. Instead, the user connects to a SmartGate Java SSL server, logs on using a Web browser form, and then accesses the applications and other privileges securely. Just as for the installed SmartPass client, the SGJC and SmartGate server generate and exchange session keys with DES/3DES encryption. Because the SGJC uses the browser and Java applet technology, the SGJC is restricted by certain non-intrusive properties of Java and the Web browser (e.g., SGJC may not be able to install the Microsoft Windows Shim layer or trap TCP/IP socket calls). Authentication is for the SGJC requires a third-party authentication method, e.g., Radius, SecurID, LDAP.

SGJC is the recommended solution for users who cannot or do not wish to install software to a desktop. It serves in situations where token storage on a hard disk poses a security threat, or where multiple users share one public computer (e.g., a public Internet kiosk or an airline pilots' lounge with one shared computer). Instead of installing any permanent keys or tokens on the client computer's hard disk, SGJC uses the SmartGate Java SSL server to automatically download a Java applet upon authentication with the SmartGate server. This applet runs within the browser's Java Runtime Environment (JRE) until the user closes the connection.

How It Works

The SGJC environment uses four components:

1. Web browser and Java applet
2. Java SSL server
3. SmartGate server(s)
4. Target applications

The Web browser and Java applet provide the functions of the traditional SmartPass client: local proxies for TCP, SOCKS proxy (UDP and TCP), session encryption, and ACL connection routing. The Java SSL server loads the Java applet, processes forms for logon, and acts as the gateway to backend SmartGate servers. SmartGate server(s) perform their traditional functions of Web proxy, TCP proxy, authentication, and Dynamic Configuration.

The SGJC Java applet emulates two protocols—SOCKS proxy and HTTP proxy. Together with the SmartGate server, these components provide a strong secure session between the end user (client) and the SmartGate server. The same security parameters and algorithms supported in the installed SmartPass scenario—i.e., DES and 3DES—are used. Ephemeral session keys are generated and exchanged between client and server. These session keys are renewed at user re-authentication or at the expiration of (an administrator-configurable) renewal timeout. If a timeout occurs, the user is prompted to re-authenticate and new keys are generated. This prevents hackers from listening in on long sessions and attempting "replay" or "code-breaking" break-ins.

The SOCKS proxy (RFC 1928) standard supports UDP relay service. SGJC emulates the SOCKS proxy protocol. UDP-based applications can use this to communicate securely to the server. Citrix Extranet Program Neighborhood (PN) uses UDP relay service to interface with its servers.

ADMINISTRATION—USER GROUP MANAGEMENT AND ACCESS CONTROL

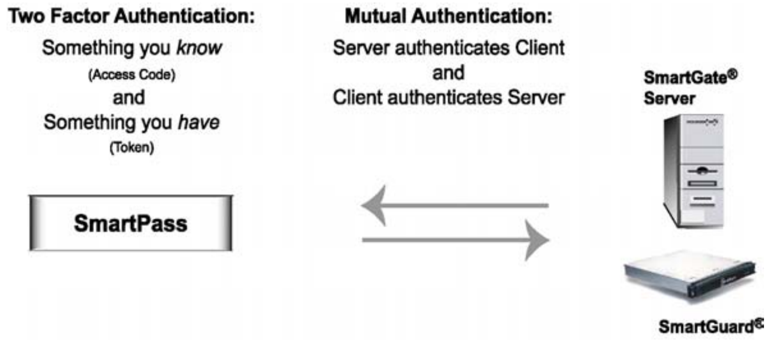
SmartGate incorporates SmartAdmin, which is a powerful and flexible Web-based administrative management utility. With SmartAdmin, administration of SmartGate users, groups, and access control lists can be centralized or distributed. There are four levels of administrator capabilities, from Superusers, who have complete control over the user community, to Observers, who have the ability to only view information. The lowest three administrator levels can be restricted to certain groups or given access to the entire user community.

Access permissions are defined as associations (TCP and IPSec services or Web resources) between users and connections. Access permissions are granted to individuals or groups. Groups can be nested inside each other. For example, the sales group can be placed in the employee group and automatically receive the permissions granted to all users in the employee group, in addition to those granted to sales. Individual exceptions can also be made. For example, one might place an external sales agent in the sales group and grant him access to the sales force automation system, but deny him access to the internal commission database. A user can belong to as many groups as practicable to administer, with unlimited numbers of nesting levels.

Remote SmartAdmin Web administration can be used by anyone with SmartPass access and administrative privileges, including wireless PDAs for ultimate portability.

AUTHENTICATION

The SmartGate Authentication Server is the final authority that determines whether any user attempting to connect via SmartGate will be granted access. It not only validates the identity of the user, but also decides whether the user's access request is legitimate. SmartGate uses mutual authentication, which means the client authenticates the server and the server authenticates the client to verify that each is communicating to the correct location. In addition, two-factor user authentication is used which employs a secret access code that the user knows and a 3DES key in the token that the user has. Access is based on authenticated user identification, independent of IP address.



SESSION ENCRYPTION

SmartGate has a dynamic session key generation capability that creates a new key for each session. The session key is generated at the time of authentication, which happens each time a user requests access to an application. The server and client engage in a challenge/response scenario with each other to establish authenticity and security for the VPN connection. This highly secure process renders pointless the key capture that is the hallmark of a certain type of hacker, because once the current session is over, the key is never used again. In addition, SmartGate's strong encryption is approved for export, without special permission, to any country that has not been embargoed by the U.S. Government.

AUDITING AND LOGGING

Auditing and logging occur continuously and automatically during a SmartPass-to-SmartGate session. These records can be reviewed in the event of suspected intrusion, reviewed periodically as a security check, or passed to another reporting server for formatting and distribution.

THE SMARTGUARD APPLIANCE

V-ONE has encapsulated its technology suite into a “drop-in” integrated VPN hardware appliance series. The SmartGuard solution combines a complete turnkey VPN that includes the V-ONE stateful inspection firewall, site-to-site IPSec, and the optional SmartGuard Command Center, the easiest management capability available today. This appliance enables V-ONE customers to quickly and easily create thousands of site-to-site VPN connections in addition to the remote access and extranet links enabled by the integrated SmartGate server technology.

The SmartGuard Command Center

Using the optional SmartGuard Command Center, an administrator can manage thousands of SmartGuard appliances throughout the world. The Command Center is a simple, secure, Web accessible VPN management utility. Using the Command Center, you have the ability to:

- Manage IPSec tunnel configurations
- Manage SmartGuard configurations
- Monitor tunnel & interface status
- View logs and state information
- Administer remote backup control
- Administer SmartGate functionality

SmartGuard also includes an optional high availability solution, which will failover automatically if a server encounters any downtime. A network consisting of multiple SmartGuard appliances automatically determines the master/slave status. The backup unit constantly checks the “heartbeat” of the primary device. All configuration information is mirrored onto the backup device, and in the event of a failure of the primary unit, an automatic failover occurs. This failover is transparent to most users and enables the continuation of service to the entire network. After the failed unit is restored, it automatically becomes the backup unit. This combination of technology comprises the following:

1. An all-in-one, fully integrated VPN solution consisting of firewall, IPSec, and application proxy technology that includes a simple configuration utility.
2. The benefits of OLR for ease of user token deployment and registration.
3. Robust IPSec site-to-site tunneling capability.

4. Powerful and easy-to-use tunnel implementation, monitoring, and management capability via the SmartGuard Command Center.
5. High availability with failover capabilities to empower large-scale deployments that are very reliable and available at all times.
6. International Computer Security Association (ICSA) certification.

CONCLUSION

Virtual private networking presents a significant opportunity for improving worldwide business communications. In order to fulfill that opportunity, VPN technology must address the security risks associated with Internet-based communications, as well as the practical management issues of deploying and servicing remote users. V-ONE technology has been helping customers deploy major VPN implementations since 1995 and has a proven track record for effectively securing large and small organizations in both wired and wireless environments.

V-ONE Corporation
20300 Century Boulevard, Suite 200
Germantown, MD 20874
1-800-495-VONE or 301-515-5200
FAX: 301-515-5280
www.v-one.com